PCT WELTORGANISATION FÜR GEISTIGES EIGENTUM
Internationales Büro

INTERNATIONALE ANMELDUNG VERÖFFENTLICHT NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT)

(51) Internationale Patentklassifikation 6 : H04L 9/32 — A1

(11) Internationale Veröffentlichungsnummer: **WO 98/47264**

(43) Internationales Veröffentlichungsdatum: 22. Oktober 1998 (22.10.98)

(21) Internationales Aktenzeichen: PCT/DE98/00563

(22) Internationales Anmeldedatum: 25. Februar 1998 (25.02.98)

(30) Prioritätsdaten:
197 15 486.7 14. April 1997 (14.04.97) DE

(71) Anmelder *(für alle Bestimmungsstaaten ausser US)*: SIEMENS AKTIENGESELLSCHAFT [DE/DE]; Wittelsbacherplatz 2, D–80333 München (DE).

(72) Erfinder; und
(75) Erfinder/Anmelder *(nur für US)*: HANCK, Martina [DE/DE]; Am Grenzweg 2, D–85635 Höhenkirchen (DE). HOFFMANN, Gerhard [DE/DE]; Gozbertstrasse 8/II, D–81547 München (DE). LUKAS, Klaus [DE/DE]; Niemöllerallee 6, D–81793 München (DE).

(81) Bestimmungsstaaten: AU, ID, JP, US, europäisches Patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

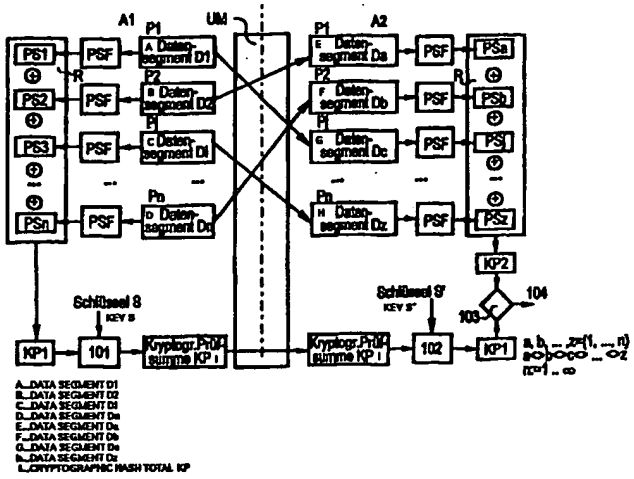
Veröffentlicht
Mit internationalem Recherchenbericht.
Vor Ablauf der für Änderungen der Ansprüche zugelassenen Frist; Veröffentlichung wird wiederholt falls Änderungen eintreffen.

(54) Title: METHOD AND SYSTEM FOR PRODUCING AND CHECKING A HASH TOTAL FOR DIGITAL DATA GROUPED IN SEVERAL DATA SEGMENTS

(54) Bezeichnung: VERFAHREN UND ANORDNUNG ZUR BILDUNG UND ÜBERPRÜFUNG EINER PRÜFSUMME FÜR DIGITALE DATEN, DIE IN MEHRERE DATENSEGMENTE GRUPPIERT SIND

(57) Abstract

The invention relates to methods and systems for producing a hash total and checking a hash total for digital data, said data being grouped into data segments. According to this method, a hash total is produced for each data segment. The individual hash totals are combined to form a first commutative hash total using a commutative link. In order to check the first commutative hash total, another hash total is produced for each data segment and these hash totals are combined to form a second commutative hash total using a commutative link. The first commutative hash total and the second commutative hash total are then checked to make sure that they coincide.



(57) Zusammenfassung

Es werden Verfahren und Anordnungen zur Bildung einer Prüfsumme und zur Überprüfung einer Prüfsumme für digitale Daten, die in mehrere Datensegmente gruppiert sind, angegeben. Bei dem Verfahren wird für jedes Datensegment eine Prüfsumme gebildet. Die einzelnen Prüfsummen werden unter Verwendung einer kommutativen Verknüpfung zu einer ersten kommutativen Prüfsumme verknüpft. Zur Überprüfung der ersten kommutativen Prüfsumme wird für jedes Datensegment wiederum eine Prüfsumme gebildet und die Prüfsumme wiederum unter Verfahren einer kommutativen Verknüpfung zu einer zweiten kommutativen Prüfsumme verknüpft. Die erste kommutative Prüfsumme und die zweite kommutative Prüfsumme werden auf Übereinstimmung überprüft.

LEDIGLICH ZUR INFORMATION

Codes zur Identifizierung von PCT-Vertragsstaaten auf den Kopfbögen der Schriften, die internationale Anmeldungen gemäss dem PCT veröffentlichen.

AL	Albanien	ES	Spanien	LS	Lesotho	SI	Slowenien
AM	Armenien	FI	Finnland	LT	Litauen	SK	Slowakei
AT	Österreich	FR	Frankreich	LU	Luxemburg	SN	Senegal
AU	Australien	GA	Gabun	LV	Lettland	SZ	Swasiland
AZ	Aserbaidschan	GB	Vereinigtes Königreich	MC	Monaco	TD	Tschad
BA	Bosnien-Herzegowina	GE	Georgien	MD	Republik Moldau	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagaskar	TJ	Tadschikistan
BE	Belgien	GN	Guinea	MK	Die ehemalige jugoslawische Republik Mazedonien	TM	Turkmenistan
BF	Burkina Faso	GR	Griechenland			TR	Türkei
BG	Bulgarien	HU	Ungarn	ML	Mali	TT	Trinidad und Tobago
BJ	Benin	IE	Irland	MN	Mongolei	UA	Ukraine
BR	Brasilien	IL	Israel	MR	Mauretanien	UG	Uganda
BY	Belarus	IS	Island	MW	Malawi	US	Vereinigte Staaten von Amerika
CA	Kanada	IT	Italien	MX	Mexiko		
CF	Zentralafrikanische Republik	JP	Japan	NE	Niger	UZ	Usbekistan
CG	Kongo	KE	Kenia	NL	Niederlande	VN	Vietnam
CH	Schweiz	KG	Kirgisistan	NO	Norwegen	YU	Jugoslawien
CI	Côte d'Ivoire	KP	Demokratische Volksrepublik Korea	NZ	Neuseeland	ZW	Zimbabwe
CM	Kamerun			PL	Polen		
CN	China	KR	Republik Korea	PT	Portugal		
CU	Kuba	KZ	Kasachstan	RO	Rumänien		
CZ	Tschechische Republik	LC	St. Lucia	RU	Russische Föderation		
DE	Deutschland	LI	Liechtenstein	SD	Sudan		
DK	Dänemark	LK	Sri Lanka	SE	Schweden		
EE	Estland	LR	Liberia	SG	Singapur		

Beschreibung

Verfahren und Anordnung zur Bildung und Überprüfung einer Prüfsumme für digitale Daten, die in mehrere Datensegmente gruppiert sind

Bei der digitalen Kommunikation, d.h. beim Austausch digitaler Daten ist es oftmals wünschenswert, die Übertragung der elektronischen Daten hinsichtlich verschiedenster Aspekte abzusichern.

Ein sehr bedeutender Aspekt ist der Schutz der zu übertragenden digitalen Daten gegen unerlaubte Modifikation, die sog. Sicherung der Integrität der Daten.

Aus [1] ist zum Schutz gegen unerlaubte Modifikation digitaler Daten die sog. kryptographische Prüfsumme bekannt, z.B. die digitale Signatur. Das in [1] beschriebene Verfahren basiert auf der Bildung eines Hashwertes aus den digitalen Nutzdaten und der anschließenden kryptographischen Bearbeitung des Hashwertes mit einem kryptographischen Schlüssel. Das Ergebnis ist eine kryptographische Prüfsumme. Zur Überprüfung der Integrität wird mit einem entsprechenden kryptographischen Schlüssel die inverse kryptographische Operation auf die gebildete Prüfsumme durchgeführt und das Ergebnis mit dem erneut aus den Nutzdaten berechneten Hashwert verglichen. Bei Übereinstimmung der ermittelten Hashwerte ist die Integrität der Nutzdaten gewährleistet.

Diese bisher übliche Vorgehensweise bedingt, daß die kompletten Nutzdaten auf Empfängerseite in identischer Reihenfolge, wie sie bei der Bildung des Hashwertes vorlagen, vorliegen müssen, da sonst die Hashwertbildung zu einem fehlerhaften Wert führt. Oftmals ist es jedoch bei der digitalen Kommunikation üblich, die zu übertragenden Nutzdaten aufgrund von Protokollrandbedingungen in kleinere Datensegmente, die auch als Datenpakete bezeichnet werden, zu unterteilen und zu

übertragen. Die Datensegmente sind oftmals nicht an eine definierte Reihenfolge gebunden oder ein definiertes sequentielles Eintreffen der Datensegmente kann nicht garantiert werden. Bei dem Verfahren aus [1] ist es also erforderlich, daß die kompletten Nutzdaten auf Empfängerseite, d.h. nach der Übertragung der Datensegmente wieder in der Reihenfolge, in der sie ursprünglich gesendet wurden, zusammengesetzt werden. Die zu übertragenden Daten können ausschließlich in dieser Reihenfolge verifiziert werden. Dies bedeutet jedoch oft einen erheblichen zusätzlichen Aufwand zur Flußkontrolle der Datensegmente, soweit dies überhaupt im Rahmen des verwendeten Protokolls möglich ist.

Aus [2] sind Grundlagen über kommutative Verknüpfungen bekannt. In [2] ist ferner eine allgemeine Definition für kommutative Verknüpfungen angegeben. Anschaulich ist unter einer kommutativen Verknüpfung eine Verknüpfung zu verstehen, bei der die Reihenfolge der Einzelverknüpfungen unwichtig ist und jede Reihenfolge der Einzelverknüpfung immer zu der gleichen Gesamtverknüpfung führt. Eine kommutative Verknüpfung kann beispielsweise eine EXOR-Verknüpfung, eine additive Verknüpfung oder auch eine multiplikative Verknüpfung sein.

Aus [3] sind ein Verfahren und eine Vorrichtung zur Erzeugung von Prüfkodesegmenten auf das Auftreten von Quelldaten hin und zur Ermittlung von Fehlern in den Quelldaten bekannt.

Somit liegt der Erfindung das Problem zugrunde, Verfahren und Anordnungen zur Bildung und Überprüfung einer ersten kommutativen Prüfsumme für digitale Daten, die in mehrere Datensegmente gruppiert sind, anzugeben, bei der eine Flußkontrolle für die einzelnen Datensegmente nicht mehr erforderlich ist.

Das Problem wird durch das Verfahren gemäß Patentanspruch 1, durch das Verfahren gemäß Patentanspruch 2, durch das Verfahren gemäß Patentanspruch 3, durch die Anordnung gemäß Patent-

anspruch 11, durch die Anordnung gemäß Patentanspruch 12 sowie durch die Anordnung gemäß Patentanspruch 13, gelöst.

Bei dem Verfahren gemäß Patentanspruch 1 wird für digitale Daten, die in mehrere Datensegmente gruppiert sind, für jedes Datensegment eine erste Segmentprüfsumme gebildet. Die gebildeten ersten Segmentprüfsummen werden durch eine kommutative Verknüpfung zu einer ersten kommutativen Prüfsumme verknüpft.

Bei dem Verfahren gemäß Patentanspruch 2 wird eine vorgegebene erste kommutative Prüfsumme, die digitalen Daten zugeordnet ist, die in mehrere Datensegmente gruppiert sind, überprüft. Dies erfolgt dadurch, daß für jedes Datensegment eine zweite Segmentprüfsumme gebildet wird und durch eine kommutative Verknüpfung der zweiten Segmentprüfsummen eine zweite kommutative Prüfsumme gebildet wird. Die zweite kommutative Prüfsumme und die erste kommutative Prüfsumme werden auf Übereinstimmung überprüft.

Bei dem Verfahren gemäß Patentanspruch 3 zur Bildung und Überprüfung einer ersten kommutativen Prüfsumme für digitale Daten, die in Datensegmente gruppiert sind, wird für jedes Datensegment eine erste Segmentprüfsumme gebildet und die ersten Segmentprüfsummen werden durch eine kommutative Verknüpfung zu einer ersten kommutativen Prüfsumme verknüpft. Für jedes Datensegment der digitalen Daten, denen die erste kommutative Prüfsumme zugeordnet ist, werden zweite Segmentprüfsummen gebildet und durch kommutative Verknüpfung der zweiten Segmentprüfsummen wird eine zweite kommutative Prüfsumme gebildet. Die zweite kommutative Prüfsumme und die erste kommutative Prüfsumme werden auf Übereinstimmung überprüft.

Die Anordnung gemäß Patentanspruch 11 weist eine Recheneinheit auf, die derart eingerichtet ist, daß für jedes Datensegment eine Segmentprüfsumme gebildet wird, und daß durch eine kommutative Verknüpfung der Segmentprüfsummen die erste kommutative Prüfsumme gebildet wird.

Die Anordnung gemäß Patentanspruch 12 weist eine Recheneinheit auf, die derart eingerichtet ist, daß für jedes Datensegment eine zweite Segmentprüfsumme gebildet wird, durch eine kommutative Verknüpfung der zweiten Segmentprüfsummen eine zweite kommutative Prüfsumme gebildet wird, und die zweite kommutative Prüfsumme (KP2) mit der ersten kommutativen Prüfsumme (KP1) auf Übereinstimmung überprüft wird.

Die Anordnung gemäß Patentanspruch 13 weist eine Recheneinheit auf, die derart eingerichtet ist, daß folgende Verfahrensschritte durchgeführt werden:
a) für jedes Datensegment wird eine Segmentprüfsumme gebildet,
b) durch eine kommutative Verknüpfung der Segmentprüfsummen wird die erste kommutative Prüfsumme gebildet,
c) für jedes Datensegment der digitalen Daten, denen die erste kommutative Prüfsumme zugeordnet ist, wird eine zweite Segmentprüfsumme gebildet,
d) durch eine kommutative Verknüpfung der zweiten Segmentprüfsummen wird eine zweite kommutative Prüfsumme gebildet, und
e) die zweite kommutative Prüfsumme wird mit der ersten kommutativen Prüfsumme auf Übereinstimmung überprüft.

Ein erheblicher Vorteil der Verfahren sowie der Anordnungen ist darin zu sehen, daß durch Verwendung einer kommutativen Verknüpfung für einzelne Prüfsummen der Datensegmente eine Flußkontrolle für die Reihenfolge der einzelnen Datensegmente nicht mehr erforderlich ist.

Es ist ferner nicht mehr erforderlich, die kompletten Nutzdaten wieder in der ursprünglichen Reihenfolge, in der die erste kommutative Prüfsumme gebildet wurde, zusammenzusetzen. Die Reihenfolge der einzelnen Datensegmente bei der Bildung der kommutativen Prüfsumme ist nicht mehr von Bedeutung.

Werden die digitalen Daten zwischen zwei Anordnungen übertragen, so ist ein weiterer Vorteil der Verfahren darin zu sehen, daß die Überprüfung der Integrität schon begonnen werden kann, bevor alle Datensegmente empfangen worden sind, da es nicht mehr erforderlich ist, die ursprüngliche Reihenfolge bei der Bildung der ersten Prüfsumme beizubehalten. Dies führt zu einer Zeitersparnis bei der Überprüfung der Integrität der Daten.

Anschaulich kann die Erfindung darin gesehen werden, daß bei mehreren Datensegmenten, die insgesamt die zu schützenden Daten darstellen, für jedes Datensegment eine Prüfsumme gebildet wird und die einzelnen Prüfsummen der Datensegmente kommutativ miteinander verknüpft werden.

Vorteilhafte Weiterbildungen der Erfindung ergeben sich aus den abhängigen Ansprüchen.

Es ist vorteilhaft, die erste kommutative Prüfsumme unter Verwendung mindestens einer kryptographischen Operation kryptographisch abzusichern.

Durch diese Weiterbildung wird erreicht, daß die kryptographische Sicherheit der Daten erheblich erhöht wird. Eine kryptographische Operation in diesem Sinne ist beispielsweise die Verschlüsselung der ersten kommutativen Prüfsumme mit einem symmetrischen oder auch mit einem asymmetrischen Verschlüsselungsverfahren, wodurch eine kryptographische Prüfsumme gebildet wird. Auf Empfängerseite wird das inverse kryptographische Verfahren zu dem kryptographischen Verfahren durchgeführt, um die kryptographische Sicherheit zu gewährleisten.

Zur Bildung einer Prüfsumme, wie sie im Rahmen des Dokuments zu verstehen ist, sind verschiedene Möglichkeiten bekannt:
-eine Prüfsumme kann durch Bildung von Hashwerten für die einzelnen Datensegmente gebildet werden;

- die Prüfsummen können auch durch sog. zyklische Codes (Cyclic Redundancy Check, CRC) gebildet werden;
- es kann ferner eine kryptographische Einwegfunktion zur Bildung der Prüfsummen für die Datensegmente verwendet werden.

Die Verfahren können vorteilhaft in verschiedenen Anwendungsszenarien eingesetzt werden.

Die Verfahren können sowohl bei der Übertragung digitaler Daten zum Schutz vor Manipulation der Daten eingesetzt werden als auch bei der Archivierung digitaler Daten in einem Rechner, in dem die erste kommutative Prüfsumme gebildet wird, und zusammen mit den zu archivierenden Daten abgespeichert wird. Die erste kommutative Prüfsumme kann bei dem Laden der digitalen Daten aus dem Archivspeicher überprüft werden, um eine Manipulation der archivierten Daten zu erkennen.

Das Verfahren kann vorteilhaft für die Sicherung digitaler Daten verwendet werden, deren Datensegmente nicht an eine Reihenfolge gebunden sind. Beispiele für solche Datensegmente sind paketorientierte Kommunikationsprotokolle, z.B. Netzmanagementprotokolle wie das Simple Network Management Protocol (SNMP) oder das Common Management Information Protocol (CMIP).

Im weiteren wird ein Ausführungsbeispiel der Erfindung anhand einer Figur näher erläutert. Auch wenn das Ausführungsbeispiel im weiteren anhand des Simple-Network-Management-Protocols (SNMP) erläutert wird, so stellt dies keine Einschränkung der Verwendbarkeit des Verfahrens dar. Das Verfahren kann immer dann eingesetzt werden wenn es gilt, eine Integritätssicherung für digitale Daten zu gewährleisten, die in mehrere Datensegmente gruppiert sind.

Die Figur zeigt zwei Anordnungen, wobei von der ersten Anordnung Datensegmente zu der zweiten Anordnung übertragen werden.

In der Figur ist eine erste Rechneranordnung A1 symbolisch dargestellt, in der Datensegmente (Di, i = 1 .. n) gespeichert sind. Die Datensegmente Di bilden zusammen die digitalen Daten, die auch als Nutzdaten bezeichnet werden, für die es gilt, die Integrität zu gewährleisten.

Sowohl die erste Rechneranordnung A1 als auch eine im weiteren beschriebene zweite Rechneranordnung A2 enthalten jeweils eine Recheneinheit R, die derart eingerichtet ist, daß die im weiteren beschriebenen Verfahrensschritte durchgeführt werden.

In der ersten Anordnung A1 sind die Datensegmente Di an Positionen Pi innerhalb des gesamten Datenstroms angeordnet. Für jedes Datensegment Di wird eine erste Segmentprüfsumme PSi unter Verwendung einer Prüfsummenfunktion PSF. Die einzelnen ersten Segmentprüfsumme PSi werden durch eine kommutative Verknüpfung, wie sie in [2] definiert und beschrieben ist, zu einer ersten kommutativen Prüfsumme KP1 verknüpft. Die kommutative Verknüpfung zwischen den einzelnen Prüfsummen PSi sind in der Figur durch ein EXOR-Zeichen $\oplus$ symbolisch dargestellt.

Die erste kommutative Prüfsumme KP1 wird einem kryptographischen Verfahren, einem symmetrischen oder asymmetrischen Verfahren, unter Verwendung eines ersten kryptographischen Schlüssels S unterzogen (Schritt 101). Das Ergebnis der kryptographischen Operation ist eine kryptographische Prüfsumme KP.

Sowohl die Datensegmente Di als auch die kryptographische Prüfsumme KP werden über ein Übertragungsmedium, vorzugsweise eine Leitung oder auch eine logischen Verbindung, die in der

Fig. durch eine Kommunikationsverbindung UM symbolisch dargestellt ist, zu einer zweiten Anordnung A2 übertragen und dort empfangen.

Die sich überkreuzenden Pfeile der Datensegmente Di in der Figur deuten an, daß durch die Übertragung der Datensegmente Di diese in einer gegenüber der Reihenfolge in der ersten Anordnung A1 verschobenen Positionen Pj (j = a .. z) empfangen werden.

So wird ein Datensegment D2 an der ersten Position P1 in der zweiten Anordnung A2 als Datensegment Da empfangen. Das Datensegment D1 wird als Datensegment Dc in der zweiten Anordnung empfangen. Das Datensegment Dn wird als empfangenes Datensegment Db in der zweiten Anordnung A2 an der zweiten Position P2 empfangen.

Entsprechend dem verwendeten Verfahren wird entweder mit dem ersten kryptographischen Schlüssel S bei Verwendung eines symmetrischen Verschlüsselungsverfahrens die inverse kryptographische Operation auf die kryptographische Prüfsumme KP ausgeführt oder bei Verwendung eines asymmetrischen kryptographischen Verfahrens unter Verwendung eines zweiten kryptographischen Schlüssels S'.

Das Ergebnis der inversen kryptographischen Operation (Schritt 102) ist bei korrekter Verschlüsselung und Entschlüsselung wiederum die erste kommutative Prüfsumme KP1.

Diese wird in der zweiten Anordnung A2 gespeichert. Für den Vergleich der nunmehr in permutierter Reihenfolge, verglichen mit der ursprünglichen Reihenfolge bei der Bildung der ersten kommutativen Prüfsumme KP1 empfangenen Datensegmente Dj, werden wiederum unter Verwendung der gleichen Prüfsummenverfahren PSF zweite Segmentprüfsummen Psj für die empfangenen Datensegmente Dj gebildet.

Die sich ergebenden zweiten Prüfsummen PSj werden wiederum kommutativ miteinander verknüpft zu einer zweiten kommutativen Prüfsummen KP2.

In einem weiteren Schritt 103 wird überprüft, ob die erste kommutative Prüfsumme KP1 mit der zweiten kommutativen Prüfsumme KP2 übereinstimmt.

Ist dies der Fall, so ist die Integrität der Datensegmente Di und somit die Integrität der gesamten digitalen Daten gewährleistet (Schritt 104), wenn die verwendeten kryptographischen Verfahren bzw. die verwendeten Verfahren zur Prüfsummenbildung die entsprechende kryptographische Sicherheit gewährleisten.

Stimmen die erste kryptographische Prüfsumme KP1 und die zweite kryptographische Prüfsumme KP2 nicht miteinander überein, so würde die Integrität der Datensegmente Di verletzt und es wird eine Manipulation der Daten festgestellt und vorzugsweise einem Benutzer des Systems gemeldet.

Die Protokolldateneinheiten PDU (Protocol Data Units) sind in SNMP derart aufgebaut, daß in der Nutzdateninformation (sog. Variable Bindings) eine Liste von Objekten (Objektidentikatoren, OID/Value-Pairs) enthalten sein kann. Die Reihenfolge der Objekte innerhalb einer PDU ist dabei nicht festgelegt, so daß eine Permutation der Objekte bei der Übertragung der PDUs zwischen der ersten Anordnung A1 und der zweiten Anordnung A2 auftreten kann. Durch die Erfindung wird es nunmehr möglich, über alle Objekte einer SNMP-PDU eine einzige kryptographische Prüfsumme zu bilden, ohne daß die Reihenfolge der Objekte bzw. der PDUs berücksichtigt werden muß.

Im weiteren werden Alternativen zu dem oben beschriebenen Ausführungsbeispiel erläutert.

Das Verfahren zur Bildung der Prüfsumme PSF kann beispielsweise ein Verfahren zur Bildung von Hashwerten sein. Es kann aber auch Verfahren zur Bildung zyklischer Codes (Cyclic-Redundancy-Check, CRC) unter Verwendung rückgekoppelter Schieberegister eingesetzt werden. Auch können kryptographische Einwegfunktionen zur Bildung der Prüfsummen PSi bzw. PSj verwendet werden.

Ferner kann die kommutative Verknüpfung zusätzlich die Eigenschaft der Assoziativität aufweisen.

Sowohl das Verfahren zur Bildung der Prüfsumme als auch das Verfahren zur Überprüfung einer Prüfsumme können unabhängig voneinander durchgeführt werden. Es kann jedoch auch gemeinsam das Verfahren zur Bildung der Prüfsumme und das Verfahren zur Überprüfung der Prüfsumme durchgeführt werden.

Es ist ferner vorgesehen, keine Übertragung digitaler Daten vorzunehmen, sondern die digitalen Daten zu archivieren, d.h. in der ersten Anordnung A1 zu speichern, gemeinsam mit der ersten kommutativen Prüfsumme KP1. Bei der Wiederverwendung der archivierten Daten, d.h. beim Laden der Datensegmente Di aus dem Speicher der ersten Anordnung A1 wird dann das Verfahren zur Überprüfung der ersten kommutativen Prüfsumme KP1, wie es oben beschrieben wurde, durchgeführt. Somit können die erste Anordnung A1 und die zweite Anordnung A2 identisch sein.

Anschaulich kann die Erfindung darin gesehen werden, daß bei mehreren Datensegmenten, die insgesamt die zu schützenden Daten darstellen, für jedes Datensegment eine Prüfsumme gebildet wird und die einzelnen Prüfsummen der Datensegmente kommutativ miteinander verknüpft werden. Dadurch wird es möglich, eine Prüfsumme zu bilden und zu überprüfen, ohne daß die Reihenfolge der Datensegmente berücksichtigt werden muß.

Im Rahmen dieses Dokuments wurden folgende Veröffentlichungen zitiert:

[1] W. Stallings, Sicherheit in Netzwerk und Internet, Prentice Hall, ISBN 3-930436-29-9, S. 203-223, 1995

[2] K.-H. Kiyek und F. Schwarz, Mathmatik für Informatiker, Teubner Verlag, ISBN 3-519-03277-X, S. 11-13, 1989

[3] DE-OS 2 048 365

Patentansprüche

1. Verfahren zur Bildung einer ersten kommutativen Prüfsumme (KP1) für digitale Daten, die in mehrere Datensegmente (Di, i = 1 .. n) gruppiert sind, durch einen Rechner,
a) bei dem für jedes Datensegment (Di) eine Segmentprüfsumme (PSi) gebildet wird, und
b) bei dem durch eine kommutative Verknüpfung (⊕) der Segmentprüfsummen (Psi) die erste kommutative Prüfsumme (KP1) gebildet wird.

2. Verfahren zur Überprüfung einer vorgegebenen ersten kommutativen Prüfsumme (KP1), die digitalen Daten zugeordnet ist, die in mehrere Datensegmente gruppiert sind, durch einen Rechner,
a) bei dem für jedes Datensegment (Dj, j = a .. z) eine zweite Segmentprüfsumme (PSj) gebildet wird,
b) bei dem durch eine kommutative Verknüpfung (⊕) der zweiten Segmentprüfsummen (Psj) eine zweite kommutative Prüfsumme (KP2) gebildet wird, und
c) bei dem die zweite kommutative Prüfsumme (KP2) mit der ersten kommutativen Prüfsumme (KP1) auf Übereinstimmung überprüft wird.

3. Verfahren zur Bildung und Überprüfung einer ersten kommutativen Prüfsumme (KP1) für digitale Daten, die in mehrere Datensegmente (Di, i = 1 .. n) gruppiert sind, durch einen Rechner,
a) bei dem für jedes Datensegment (Di) eine Segmentprüfsumme (PSi) gebildet wird,
b) bei dem durch eine kommutative Verknüpfung (⊕) der Segmentprüfsummen (Psi) die erste kommutative Prüfsumme (KP1) gebildet wird,
c) bei dem für jedes Datensegment (Dj, j = a .. z) der digitalen Daten, denen die erste kommutative Prüfsumme (KP1) zugeordnet ist, eine zweite Segmentprüfsumme (PSj) gebildet wird,

d) bei dem durch eine kommutative Verknüpfung (⊕) der zweiten Segmentprüfsummen (Psj) eine zweite kommutative Prüfsumme (KP2) gebildet wird, und

e) bei dem die zweite kommutative Prüfsumme (KP2) mit der ersten kommutativen Prüfsumme (KP1) auf Übereinstimmung überprüft wird.

4. Verfahren nach einem der Ansprüche 1 bis 3,
bei dem die Segmentprüfsummen (Psi, Psj) nach mindestens einer der folgenden Arten gebildet werden:
- Hashwertbildung,
- Bildung von CRC-Codes,
- Verwendung mindestens einer kryptographischen Einwegfunktion.

5. Verfahren nach einem der Ansprüche 1 bis 4,
bei dem die erste kommutative Prüfsumme (KP1) unter Verwendung mindestens einer kryptographischen Operation kryptographisch gesichert wird.

6. Verfahren nach Anspruch 5,
bei dem die kryptographische Operation ein symmetrisches kryptographisches Verfahren ist.

7. Verfahren nach Anspruch 5,
bei dem die kryptographische Operation ein asymmetrisches kryptographisches Verfahren ist.

8. Verfahren nach einem der Ansprüche 1 bis 7,
bei dem die kommutative Verknüpfung (⊕) die Eigenschaft der Assoziativität aufweist.

9. Verfahren nach einem der Ansprüche 1 bis 8, bei dem digitale Daten gesichert werden, deren Datensegmente (Di) nicht an eine Reihenfolge gebunden sind.

10. Verfahren nach einem der Ansprüche 1 bis 8, bei dem digitale Daten gesichert werden, die nach einem Netzmanagement-Protokoll verarbeitet werden.

11. Anordnung zur Bildung einer ersten kommutativen Prüfsumme (KP1) für digitale Daten, die in mehrere Datensegmente (Di, i = 1 .. n) gruppiert sind,
mit einer Recheneinheit, die derart eingerichtet ist, daß
a) für jedes Datensegment (Di) eine Segmentprüfsumme (PSi) gebildet wird, und
b) durch eine kommutative Verknüpfung (⊕) der Segmentprüfsummen (Psi) die erste kommutative Prüfsumme (KP1) gebildet wird.

12. Anordnung zur Überprüfung einer vorgegebenen ersten kommutativen Prüfsumme (KP1), die digitalen Daten zugeordnet ist, die in mehrere Datensegmente gruppiert sind,
mit einer Recheneinheit, die derart eingerichtet ist, daß
a) für jedes Datensegment (Dj, j = a .. z) eine zweite Segmentprüfsumme (PSj) gebildet wird,
b) durch eine kommutative Verknüpfung (⊕) der zweiten Segmentprüfsummen (Psj) eine zweite kommutative Prüfsumme (KP2) gebildet wird, und
c) die zweite kommutative Prüfsumme (KP2) mit der ersten kommutativen Prüfsumme (KP1) auf Übereinstimmung überprüft wird.

13. Anordnung zur Bildung und Überprüfung einer ersten kommutativen Prüfsumme (KP1) für digitale Daten, die in mehrere Datensegmente (Di, i = 1 .. n) gruppiert sind,
mit mindestens einer Recheneinheit, die derart eingerichtet ist, daß
a) für jedes Datensegment (Di) eine Segmentprüfsumme (PSi) gebildet wird,
b) durch eine kommutative Verknüpfung (⊕) der Segmentprüfsummen (Psi) die erste kommutative Prüfsumme (KP1) gebildet wird,

c) für jedes Datensegment (Dj, j = a .. z) der digitalen Daten, denen die erste kommutative Prüfsumme (KP1) zugeordnet ist, eine zweite Segmentprüfsumme (PSj) gebildet wird,

d) durch eine kommutative Verknüpfung (⊕) der zweiten Segmentprüfsummen (Psj) eine zweite kommutative Prüfsumme (KP2) gebildet wird, und

e) die zweite kommutative Prüfsumme (KP2) mit der ersten kommutativen Prüfsumme (KP1) auf Übereinstimmung überprüft wird.

14. Anordnung nach einem der Ansprüche 11 bis 13,
bei der die Recheneinheit derart eingerichtet ist, daß die Segmentprüfsummen (Psi, Psj) nach mindestens einer der folgenden Arten gebildet werden:
- Hashwertbildung,
- Bildung von CRC-Codes,
- Verwendung mindestens einer kryptographischen Einwegfunktion.

15. Anordnung nach einem der Ansprüche 11 bis 14,
bei der die Recheneinheit derart eingerichtet ist, daß die erste kommutative Prüfsumme (KP1) unter Verwendung mindestens einer kryptographischen Operation kryptographisch gesichert wird.

16. Anordnung nach Anspruch 15,
bei der die Recheneinheit derart eingerichtet ist, daß die kryptographische Operation ein symmetrisches kryptographisches Verfahren ist.

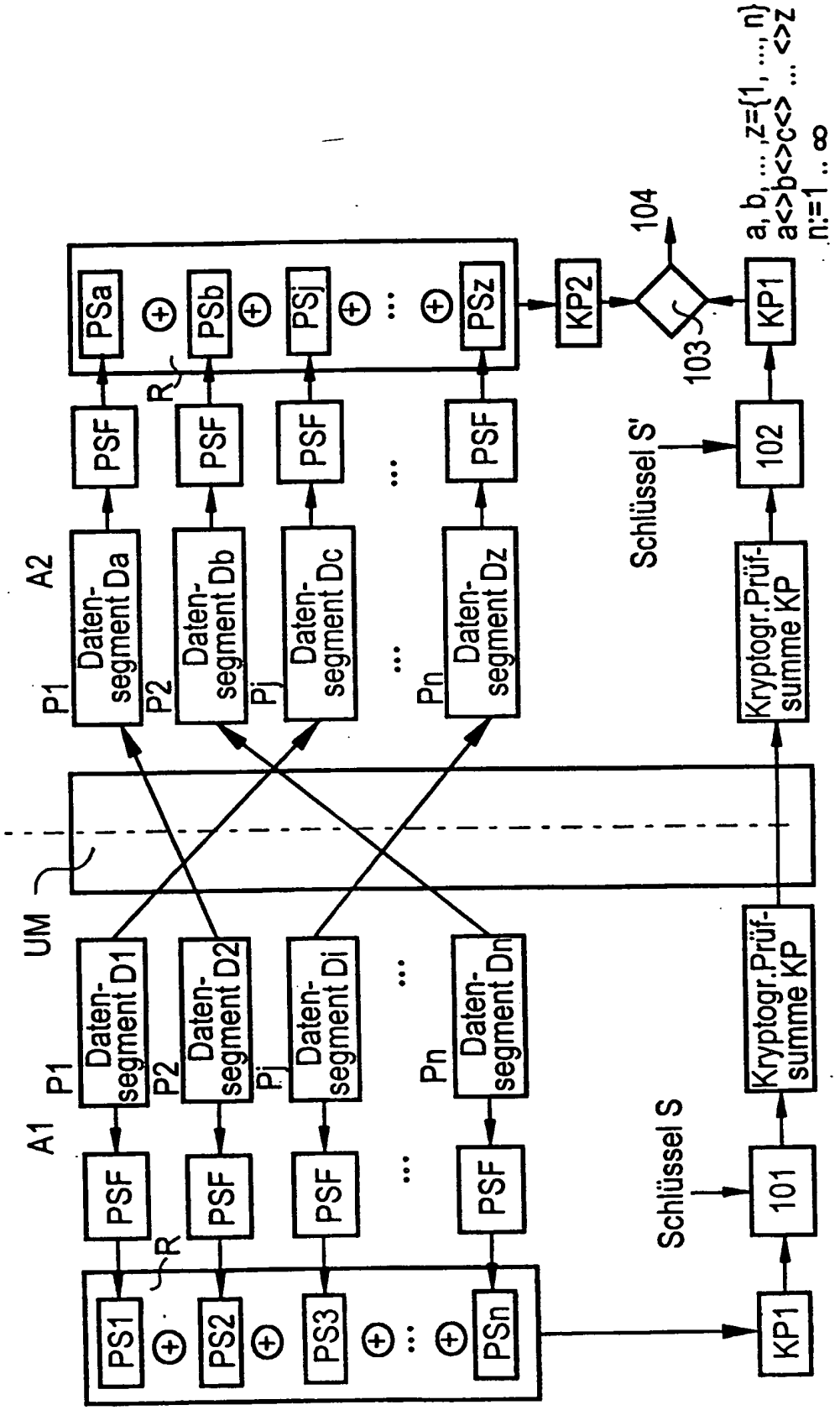
17. Anordnung nach Anspruch 15,
bei der die Recheneinheit derart eingerichtet ist, daß die kryptographische Operation ein asymmetrisches kryptographisches Verfahren ist.

18. Anordnung nach einem der Ansprüche 11 bis 17,

bei der die Recheneinheit derart eingerichtet ist, daß die kommutative Verknüpfung ($\oplus$) die Eigenschaft der Assoziativität aufweist.

19. Anordnung nach einem der Ansprüche 11 bis 18, bei der die Recheneinheit derart eingerichtet ist, daß digitale Daten gesichert werden, deren Datensegmente (Di) nicht an eine Reihenfolge gebunden sind.

20. Anordnung nach einem der Ansprüche 11 bis 18, bei der die Recheneinheit derart eingerichtet ist, daß digitale Daten gesichert werden, die nach einem Netzmanagement-Protokoll verarbeitet werden.


a, b, ..., z={1, ..., n}
a<>b<>c<> ... <>z
n:=1 .. ∞
104
103
KP2
KP1
PSa
PSb
PSj
PSz
PSF
R
A2
P1
P2
Pj
Pn
Daten-segment Da
Daten-segment Db
Daten-segment Dc
Daten-segment Dz
Schlüssel S'
102
Kryptogr.Prüf-summe KP
UM
A1
Daten-segment D1
Daten-segment D2
Daten-segment Di
Daten-segment Dn
Schlüssel S
101
PS1
PS2
PS3
PSn

INTERNATIONAL SEARCH REPORT

Inte onal Application No
PCT/DE 98/00563

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 H04L9/32

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	JP 06 315 027 A (IBM) 8 November 1994	1-4, 11-14
A	see the whole document	6,16
P,X	& US 5 673 318 A (IBM) 30 September 1997	1-4, 11-14
A	see abstract see column 1, line 63 - column 2, line 30 see column 5, line 8 - column 6, line 22 see column 5, line 8 - column 6, line 22	6,16
X	EP 0 609 595 A (HEWLETT-PACKARD) 10 August 1994 see page 3, line 28 - line 35 see page 5, line 2 - line 37 see page 3, line 52 - page 4, line 12	1-4, 11-14

-/—

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
10 August 1998	14/08/1998

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Holper, G

2

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

International Application No
PCT/DE 98/00563

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	EP 0 654 920 A (FISCHER) 24 May 1995 see abstract see column 9, line 54 - column 10, line 5 see column 10, line 44 - line 58	1,5-8, 11,15-18

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

information on patent family members

Inter nal Application No
PCT/DE 98/00563

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
JP 6315027 A	08-11-1994	US 5757913 A	26-05-1998
		US 5673318 A	30-09-1997
EP 609595 A	10-08-1994	JP 7015354 A	17-01-1995
		US 5778013 A	07-07-1998
EP 654920 A	24-05-1995	US 5475826 A	12-12-1995
		AU 3525397 A	11-12-1997
		AU 5778394 A	25-05-1995
		CA 2120678 A	20-05-1995
		JP 8083046 A	26-03-1996
		US 5694569 A	02-12-1997

INTERNATIONALER RECHERCHENBERICHT

Inte ionales Aktenzeichen
PCT/DE 98/00563

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
IPK 6 H04L9/32

Nach der Internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
IPK 6 H04L

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	JP 06 315 027 A (IBM) 8. November 1994	1-4, 11-14
A	siehe das ganze Dokument	6,16
P,X	& US 5 673 318 A (IBM) 30. September 1997	1-4, 11-14
A	siehe Zusammenfassung siehe Spalte 1, Zeile 63 - Spalte 2, Zeile 30 siehe Spalte 5, Zeile 8 - Spalte 6, Zeile 22 siehe Spalte 5, Zeile 8 - Spalte 6, Zeile 22	6,16

-/--

[X] Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen

[X] Siehe Anhang Patentfamilie

* Besondere Kategorien von angegebenen Veröffentlichungen :
"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist
"E" älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist
"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)
"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht
"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist
"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist
"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden
"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist
"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche	Absendedatum des internationalen Recherchenberichts
10. August 1998	14/08/1998

Name und Postanschrift der Internationalen Recherchenbehörde	Bevollmächtigter Bediensteter
Europäisches Patentamt, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Holper, G

2

Formblatt PCT/ISA/210 (Blatt 2) (Juli 1992)

INTERNATIONALER RECHERCHENBERICHT

Intls Jonales Aktenzeichen
PCT/DE 98/00563

C.(Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	EP 0 609 595 A (HEWLETT-PACKARD) 10. August 1994 siehe Seite 3, Zeile 28 - Zeile 35 siehe Seite 5, Zeile 2 - Zeile 37 siehe Seite 3, Zeile 52 - Seite 4, Zeile 12	1-4, 11-14
A	EP 0 654 920 A (FISCHER) 24. Mai 1995 siehe Zusammenfassung siehe Spalte 9, Zeile 54 - Spalte 10, Zeile 5 siehe Spalte 10, Zeile 44 - Zeile 58	1,5-8, 11,15-18

Formblatt PCT/ISA/210 (Fortsetzung von Blatt 2) (Juli 1992)

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Ints onales Aktenzeichen
PCT/DE 98/00563

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
JP 6315027 A	08-11-1994	US 5757913 A	26-05-1998
		US 5673318 A	30-09-1997
EP 609595 A	10-08-1994	JP 7015354 A	17-01-1995
		US 5778013 A	07-07-1998
EP 654920 A	24-05-1995	US 5475826 A	12-12-1995
		AU 3525397 A	11-12-1997
		AU 5778394 A	25-05-1995
		CA 2120678 A	20-05-1995
		JP 8083046 A	26-03-1996
		US 5694569 A	02-12-1997